# GIẢI PHÁP PHÂN PHỐI KHÓA LƯỢNG TỬ KHÔNG DÂY LAI GHÉP FSO VÀ MMW

**Phạm Anh Thư, Đặng Thế Ngọc**
Học viện Công nghệ Bưu chính Viễn thông

***Tóm tắt***—Trong bài báo này, chúng tôi đề xuất một giải pháp phân phối khóa lượng tử không dây lai ghép FSO và MMW. Khóa lượng tử từ bên gửi (Alice) được truyền qua kênh FSO tới trạm gốc (BS) và sau đó được chuyển tiếp tới các trạm di động (Bob) qua kênh vô tuyến. Giao thức QKD được thực hiện dựa trên điều chế cường độ sóng mang con (SIM) sử dụng khóa dịch pha nhị phân (BPSK) để mã hóa và bộ thu hai ngưỡng để giải mã. Hiệu năng của hệ thống QKD đề xuất được phân tích thông qua tham số tỉ lệ lỗi bit lượng tử (QBER) dưới ảnh hưởng của các tham số lớp vật lý đến từ bộ thu, kênh FSO và kênh vô tuyến MMW. Các kết quả tính toán số đã khẳng định tính khả thi trong việc triển khai hệ thống QKD đã đề xuất.

***Từ khóa***— Phân phối khóa lượng tử (QKD), truyền thông quang qua không gian (FSO- Free Space Optics), điều chế cường độ sóng mang con (SIM), tỉ lệ lỗi bit lượng tử (QBER).

## I. GIỚI THIỆU CHUNG

Việc bảo mật thông tin ngày càng được quan tâm, đặc biệt là những thông tin được truyền qua cơ sở hạ tầng mạng Internet không được bảo mật. Phương pháp bảo mật phổ biến nhất là sử dụng khóa mật mã hóa bí mật dựa trên các thuật toán mật mã. Trong phương pháp này, bên gửi hợp pháp (Alice) và bên nhận hợp pháp (Bob) phải chia sẻ khóa bí mật qua kênh công khai không an toàn [1]. Tuy nhiên, vấn đề nằm trong việc phân phối khóa nghĩa là làm sao hai bên gửi và nhận phải thông báo một cách bảo mật cho nhau về khóa bí mật được sử dụng để mã hóa thông tin. Để giải quyết được vấn đề này, rất nhiều giao thức phân phối khóa đã được đề xuất. Một trong những giao thức phân phối khóa nhận được nhiều sự quan tâm hiện nay là giao thức phân phối khóa lượng tử (QKD), trong đó hai bên gửi và nhận có thể trao đổi khóa bí mật qua kênh lượng tử, thậm chí cả khi có mặt của bên nghe trộm thứ ba (Eve) [2],[3].

Hai kênh được sử dụng trong hệ thống QKD bao gồm: kênh lượng tử và kênh công khai. Kênh lượng tử được sử dụng để truyền thông tin về khóa bí mật, được gọi là các bit lượng tử (qubit). Sau đó, xác nhận khóa sẽ được trao đổi qua một kênh khác để thống nhất về khóa bí mật dùng chung.

Giao thức QKD đầu tiên được đề xuất bởi Bennett và Brassard vào năm 1984, còn được gọi là giao thức BB84 [2]. Vào năm 1991, giao thức QKD khác được đề xuất bởi Artur Ekert, đó là giao thức E91 [4]. Các giao thức phân phối khóa này dựa trên việc mã hóa thông tin lên các biến rời rạc (DV) như pha hay phân cực của photon. Nhược điểm của các giao thức này là tốc độ và hiệu quả của việc tách sóng từng photon tại phía thu bị hạn chế. Ngược lại, giao thức QKD cũng cho phép mã hóa thông tin khóa trên các biến liên tục như biên độ hay pha của xung ánh sáng được điều chế (CV-QKD) [5]. Giao thức CV-QKD đã nhận được rất nhiều sự quan tâm từ các nhà nghiên cứu trên thế giới do tính tương thích với các mạng thông tin quang và tốc độ trao đổi khóa khá cao.

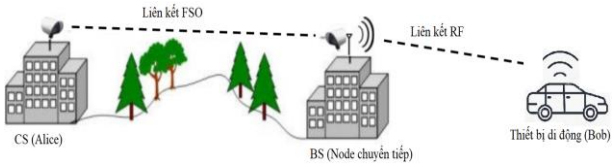
Để phân phối khóa bí mật sử dụng giao thức DV/CV-QKD giữa Alice và Bob, các môi trường truyền dẫn khác nhau gồm mạng truyền thông sợi quang [6],[7], truyền thông quang qua không gian (FSO) dưới mặt đất [8],[9] và FSO dựa trên vệ tinh [10],[11] đã được nghiên cứu một cách rộng rãi. Trong khi, phương pháp phân phối khóa lượng tử dựa trên sợi quang đã được nghiên cứu và rất nhiều ứng dụng đã được triển khai, nhưng đây chỉ là phương pháp sử dụng cho các đầu cuối cố định. Tuy nhiên, có rất nhiều ứng dụng thực tế, bao gồm cả trong đời sống hàng ngày hay trong quân đội, mà trong đó đầu cuối sử dụng là các thiết bị di động, ví dụ như các mạng xe cộ, đòi hỏi các giải pháp QKD vô tuyến. Trong bối cảnh đó, FSO, một hệ thống dễ thực thi và có chi phí hợp lý, có thể được sử dụng để truyền khóa lượng tử tới các trạm di động [12]. Kết quả là, hệ thống QKD dựa trên FSO đã nhận được rất nhiều sự quan tâm gần đây, bao gồm cả hệ thống mặt đất [13]-[15] và hệ thống vệ tinh [16]-[18].

Cũng như các hệ thống FSO khác, hệ thống QKD dựa trên FSO chịu rất nhiều ảnh hưởng của môi trường khí quyển như hấp thụ, tán xạ,... làm hạn chế khoảng cách truyền dẫn [13]. Do vậy, sử dụng trạm chuyển tiếp là một giải pháp đã được đề xuất để mở rộng khoảng cách hoạt động của các hệ thống này [19]. Mặt khác, việc sử dụng kênh FSO yêu cầu sử dụng các kỹ thuật phức tạp cho việc căn chỉnh và bám để duy trì kết nối tầm nhìn thẳng (LOS) giữa bên phát và bên thu. Trong khi đó, kết nối không dây ở băng tần vô tuyến (RF) có thể phục vụ các trạm di động

Tác giả liên lạc: Đặng Thế Ngọc
Email: ngocdt@ptit.edu.vn
Đến tòa soạn: 4/2020, chỉnh sửa: 6/2020, chấp nhận đăng: 7/2020.

tốt hơn. Nhưng vấn đề đặt ra là việc thực thi giao thức QKD trên hệ thống vô tuyến RF cũng là một thách thức [2].

Trong bài báo này, mô hình hệ thống phân phối khóa lượng tử không dây lai ghép FSO và MMW được đề xuất. Ưu điểm của kiến trúc đề xuất này là có thể cung cấp tốc độ truyền dẫn cao hơn, mềm dẻo hơn và có khả năng mở rộng. Hệ thống phân phối khóa QKD đề xuất có thể được ứng dụng cho các mạng di động trong việc phân phối khóa bí mật từ các trạm trung tâm (CS) tới các nút di động (MN) trong đó BS sẽ đóng vai trò là node chuyển tiếp. Liên kết FSO trong mô hình này được sử dụng để kết nối CS và BS trong khi giữa BS và MN là các liên kết vô tuyến RF ở băng sóng MMW (Hình 1). Do giao thức QKD mã hóa thông tin khóa trên photon hoặc xung ánh sáng không thể được thực thi trên liên kết RF, chúng tôi đề xuất sử dụng điều chế cường độ sóng mang con (SIM) với kỹ thuật điều chế BPSK cho phần liên kết FSO. Thông tin khóa sẽ được mang bởi sóng mang con RF qua liên kết FSO (RoFSO). Hiệu năng về tỉ lệ lỗi bit lượng tử (QBER) của hệ thống QKD đề xuất được phân tích dưới ảnh hưởng của rất nhiều các tham số lớp vật lý đến từ bộ thu, liên kết FSO và kênh vô tuyến.




*Hình 1.* Mô hình hệ thống QKD không dây lai ghép FSO và MMW.

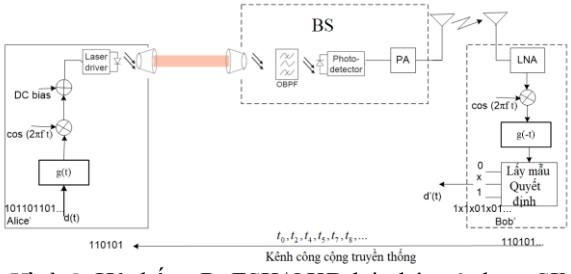
Phần còn lại của bài báo được bố cục như sau. Mô hình hệ thống đề xuất được giới thiệu trong phần 2. Trong phần 3, chúng tôi sẽ xây dựng công thức phân tích hiệu năng của hệ thống về mặt tỉ lệ lỗi bit lượng tử và tốc độ khóa bí mật. Phần 4 trình bày các kết quả tính toán số và các đánh giá về các kết quả này. Cuối cùng, phần 5 sẽ là phần kết luận của bài báo.

## II. MÔ HÌNH HỆ THỐNG

Giao thức QKD được thực hiện trong hệ thống đề xuất được dựa trên SIM sử dụng khóa dịch pha nhị phân (SIM-BPSK), đây là mô hình điều chế đã được sử dụng thành công cho hệ thống FSO [9]. Sơ đồ khối của hệ thống RoFSO/QKD đề xuất được chỉ ra trong hình 2. Hệ thống đề xuất bao gồm ba phần chính, trạm trung tâm phân phối khóa, trạm chuyển tiếp tại BS, và thiết bị di động là nơi nhận khóa.

Tại trạm trung tâm (bộ phát của Alice), các bit nhị phân của khóa được chuyển sang hàm dạng xung chữ nhật (g(t)) và được điều chế lên sóng mang con RF sử dụng điều chế BPSK, trong đó bit "0" và "1" được biểu diễn bằng hai phai cách nhau 180 độ. Tiếp theo, tín hiệu BPSK, bao gồm cả giá trị âm và dương, được cộng thêm dòng định thiên DC vào trước khi điều chế với sóng quang liên tục được tạp ra bởi LD. LD chỉ có thể được điều chế bởi các tín hiệu dương nên tín hiệu BPSK phải cộng thêm với dòng DC trước khi đưa vào điều chế. Sau đó, tín hiệu quang được truyền qua không gian tới BS. Tại BS, tín hiệu được đưa qua bộ tách sóng APD và bộ khuếch đại công suất PA. Đầu ra tại BS là sóng mang RF được điều chế BPSK sẽ được truyền trên kênh vô tuyến tới node di động, đây chính là bộ thu của Bob.

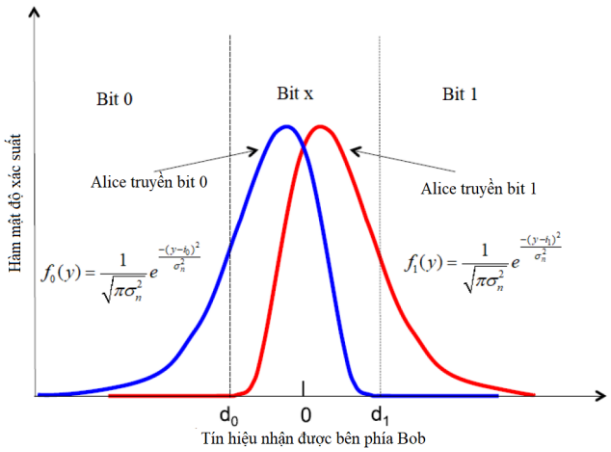
Tại phía thu (Bob), tín hiệu thu được trước tiên được khuếch đại bởi bộ khuếch đại tạp âm thấp LNA. Sau đó, tín hiệu được khuếch đại và giải điều chế bằng cách nhân với tín hiệu đến từ bộ dao động nội có tần số là tần số của sóng mang con vô tuyến. Sau khi giải mã, tín hiệu điện được qua bộ chỉnh xung (g(-t)), lấy mẫu và được quyết định là các bit "0", "1", hay "x" dựa trên bộ tách sóng hai ngưỡng (DT). Như chỉ ra trong hình 3, hai mức ngưỡng $d_0$ và $d_1$, được thiết lập tại phía Bob cho việc tách sóng tín hiệu. Nếu dòng tín hiệu nhận được nhỏ hơn $d_0$, bit "0" sẽ được quyết định. Nếu dòng tín hiệu nhận được lớn hơn $d_1$, bit "1" sẽ được quyết định. Trường hợp còn lại, bit "x" (không bit nào) được tạo ra.



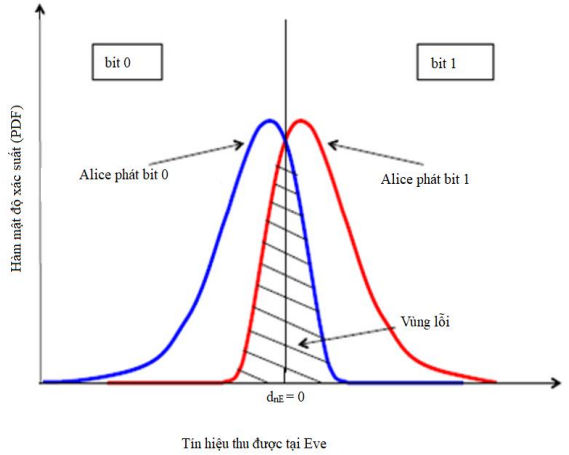

*Hình 2.* Hệ thống RoFSK/QKD lai ghép sử dụng SIM-BPSK và bộ thu DT/DD.

Cuối cùng, Bob thông báo cho Alice biết các thời điểm mà các bit "0" và "1" được tạo ra qua kênh công cộng truyền thống. Sau đó Alice loại bỏ các giá trị bit tại thời điểm mà Bob không tạo ra bit. Từ đây, Alice và Bob chia sẻ một chuỗi bit giống hệt nhau, gọi là khóa chọn lọc. Căn cứ vào thông tin trạng thái kênh CSI tại máy thu, $d_0$ và $d_1$ có thể được điều chỉnh, do đó xác suất chọn lọc tại máy thu của Bob có thể được điều khiển.

Tính an ninh của ý tưởng thiết kế này có thể được giải thích như sau. Thứ nhất, độ sâu điều chế δ của các tín hiệu SIM/BPSK được chọn là đủ nhỏ để Eve không thể phân biệt hoàn toàn trạng thái được phát. Eve cũng có thể cố gắng sử dụng ngưỡng kép D-T như Bob, tuy nhiên, sự thăng giáng tín hiệu của Eve không tương quan với tín hiệu của Bob, do đó các bit khóa được tạo ra bởi Bob và Eve tạo ra không khớp nhau. Nếu Eve cố giải mã khóa bằng cách sử dụng ngưỡng tối ưu (là $d_{nE}$ tại "không" như trong hình 4), nó thu được các giá trị đo trong đó hai tín hiệu bị chồng chéo nhiều lên nhau, vì vậy nó sẽ phải chịu một tỷ lệ lỗi cao, do đó làm giảm sự hiểu biết về khóa có lợi cho Eve. Thứ hai, xác suất chọn lọc cũng có thể được điều khiển bởi Bob thông qua thiết lập ngưỡng kép D-T. Điều này có nghĩa là lượng thông tin được chia sẻ giữa Alice và Bob có thể được kiểm soát. Kết quả là, chúng ta có thể đảm bảo tỷ lệ bí mật tích cực bằng cách điều chỉnh độ sâu điều chế và cài đặt D-T đúng cách để thông tin tương hỗ giữa Alice và Bob luôn lớn hơn thông tin Eve thu được theo các chiến lược nghe lén khác nhau.




*Hình 3.* Tách sóng hai ngưỡng tại phía Bob.




*Hình 4.* Hàm mật độ xác suất của tín hiệu thu của Eve trên kênh pha-đinh với ngưỡng tối ưu $d_{nE}$.

## III. HIỆU NĂNG HỆ THỐNG ĐỀ XUẤT

Trong phần này, dòng tín hiệu và nhiễu tại phía thu của Bob được tính toán trước. Sau đó, hiệu năng của hệ thống về mặt tỉ lệ lỗi bit lượng tử (QBER) được tính dựa trên xác suất lỗi và số bit khóa được sử dụng. Hơn nữa, tốc độ khóa bí mật cũng sẽ được xem xét trong phần này.

### 3.1. Tín hiệu thu và nhiễu

Như chỉ ra trong mô hình hệ thống (Hình 2), các bit khóa, chuỗi các bit nhị phân ngẫu nhiên "0" hoặc "1", được điều chế BPSK với sóng mang, sau đó được biến đổi thành tín hiệu quang nhờ điều chế cường độ với độ sâu điều chế nhỏ [13]. Công suất thu được của chùm laser được điều chế có thể biểu diễn như sau:

$$P_t(t)=\frac{P_p}{2}\left[1+mS(t)\right] \quad (1)$$

trong đó, $P_p$ là công suất phát đỉnh, $m$ là độ sâu điều chế cường độ với $0 < m < 1$. $S_t(t) = A(t)g(t)\cos(2\pi f_c t + a_i\pi)$, trong đó $A(i)$ biên độ sóng mang, $g(t)$ hàm tạo xung chữ nhật, $f_c$ là tần số sóng mang và $a_i \in \{0,1\}$ là bit nhị phân thứ $i$. Trước khi được truyền qua kênh FSO, tín hiệu quang phát sẽ được khuếch đại bởi thấu kính phát với hệ số khuếch đại là $G_{TX}^{CS}$.

Tại BS, tín hiệu quang thu tại đầu ra của thấu kính thu có hệ số khuếch đại là $G_{RX}^{BS}$ sẽ được chuyển qua bộ lọc thông dải quang (OBPF) và được biến đổi ngược lại thành tín hiệu điện nhờ bộ tách sóng APD. Dòng tín hiệu điện sau APD có thể được mô tả như sau:

$$i_p(t)=\Re M_A\frac{\sqrt{P_r^{BS}}}{2}\left[1+mS(t)\right]+n_{BS}(t), \quad (2)$$

trong đó, $\Re$ và $M_A$ tương ứng là đáp ứng và hệ số khuếch đại của APD, $n_{BS}(t)$ là dòng nhiễu tại bộ thu tại BS. $P_r^{BS}$ là công suất thu đỉnh tại BS được tính bởi:

$$P_r^{BS}=P_p G_{TX}^{CS} P_L^F h_F G_{RX}^{BS} G_A, \quad (3)$$

trong đó $P_L^F=\left(4\pi L/\lambda\right)^2$ là suy hao không gian tự do của kênh FSO giữa CS và BS với $L$ là khoảng cách từ CS tới BS, $h_F$ là tham số trạng thái kênh FSO đặc trưng cho suy hao khí quyển và hình học của kênh truyền FSO, và $G_A$ là hệ số khuếch đại của bộ khuếch đại công suất (PA).

Nhiễu tại BS bao gồm nhiễu cường độ tương đối (RIN) của bộ khuếch đại và nhiễu bộ thu bao gồm nhiễu nhiệt vào nhiễu nổ. Biến thiên nhiễu tại BS có thể được biểu diễn như sau:

$$\sigma_{BS}^2=2qM_A^2F_A\Re m\frac{P_r^{BS}}{4}B_n+\frac{KTB_n}{R_L}F_n, \quad (4)$$
$$+2S_{RIN}\left(\Re M_A m P_r^{BS}\right)^2 B_n$$

trong đó, $q$ là điện tích electron, $B_n = R_b/2$ là băng tần nhiễu hiệu dụng, $R_b$ tốc độ bit, $K$ là hằng số Boltzmann, $T$ là nhiệt độ Kelvin, $R_L$ điện trở tải, $F_n$ là hệ số nhiễu của bộ khuếch đại công suất PA, và $F_A(M_A) = k_A M_A + (1- k_A)(2-1/M_A)$ là hệ số nhiễu trội của APD, trong đó $k_A$ là tỉ lệ ion hóa nhận giá trị từ 0 đến 1 [21]. $S_{RIN}$ là mật độ phổ công suất của nhiễu RIN.

Sau đó, tín hiệu RF từ BS được truyền tới bên phía thu của Bob, tại đây tín hiệu BPSK được giải điều chế bằng cách trộn với tín hiệu từ bộ dao động nội có dạng $\cos(2\pi f_c t)$. Dòng tín hiệu sau giải điều chế có thể được biểu diễn là:

$$i_d(t)=i_p(t)\sqrt{h_w}\cos\left(2\pi f_c t\right)+n_{MN}(t), \quad (5)$$

trong đó, $h_w$ là hệ số kênh của kênh vô tuyến. $n_{MN}(t)$ là nhiễu tại bộ thu tại bên thu có biến thiên là $\sigma_{MN}^2=KTB_n/R_L$. Bằng cách sử dụng bộ lọc thông thấp để loại bỏ các thành phần tần số cao như $f_c$ hay $2f_c$, tín hiệu băng gốc có thể thu được tại đầu ra của bộ lọc LPF được xác định bởi:

$$r(t)=\begin{cases} i_0=-\frac{1}{4}\Re M_A\sqrt{P_r^{BS}}m\sqrt{h_w} \\ \quad +n_{BS}(t)\sqrt{h_w}+n_{MN}(t) \\ i_1=+\frac{1}{4}\Re M_A\sqrt{P_r^{BS}}m\sqrt{h_w} \\ \quad +n_{BS}(t)\sqrt{h_w}+n_{MN}(t) \end{cases}, \quad (6)$$

trong đó, $i_0$ và $i_1$ là tín hiệu nhận được tương ứng với bit "0" và "1". Tổng phương sai nhiễu được tính như sau $\sigma_n^2=\sigma_{BS}^2h_w+\sigma_{MN}^2$. Tiếp theo, tín hiệu sau giải điều chế được chuyển tới bộ tách sóng hai ngưỡng để quyết định

bit nhận được là "0", "1", hay "x" như trong hình 3.

### 3.2. Mô hình kênh

Trong phần này, mô hình của kênh FSO từ CS tới BS và kênh RF từ BS tới các thiết bị đầu cuối di động sẽ được xem xét.

Trong kênh FSO, tham số trạng thái kênh FSO đặc trưng cho suy hao của kênh truyền FSO ( $h_F$ ) bao gồm ba thành phần: suy hao đường truyền $h_L$ ; tổn hao hình học và lệch hướng $h_p$. Để đơn giản, trong bài báo này chúng tôi bỏ qua thành phần nhiễu loạn không khí. Theo đó, trạng thái kênh FSO có thể biểu diễn như sau:

$$h_F = h_L h_P . \quad (7)$$

Suy hao của tín hiệu trong bầu khí quyển là hệ quả của quá trình hấp thụ và tán xạ. Với một tuyến FSO trên mặt đất, cường độ tín hiệu thu được tại khoảng cách $L$ từ bộ phát có quan hệ với cường độ tín hiệu phát theo quy luật Beer – Lambert như sau:

$$h_L = \exp(-a_L L) . \quad (8)$$

trong đó $a_L$ (tính theo đơn vị $m^{-1}$) là hệ số suy hao.

Để đánh giá suy hao tín hiệu do ảnh hưởng của sự lệch hướng, búp sóng quang được mô hình hóa theo mô hình phân bố Gauss với phân bố cường độ tín hiệu phát chuẩn hóa theo không gian tại khoảng cách $L$ từ bộ phát xác định theo:

$$I_{beam}(\rho;\mathrm{L}) = \frac{2}{\pi\omega_L^2}\exp\left(-\frac{2\mathrm{P}\rho\mathrm{P}^2}{\omega_L^2}\right), \quad (9)$$

với $\rho$ là vec-tơ bán kính từ tâm búp sóng quang, và $\omega_L$ là độ rộng búp sóng quang (bán kính búp sóng Gauss tính tại $e^{-2}$) tại khoảng cách $L$ [23].

Tổn hao hình học do sự mở rộng búp sóng tại phía thu kết hợp với ảnh hưởng của lệch hướng được xác định:

$$h_p(r;L) = \int_A I_{beam}(\rho - r;L)d\rho , \quad (10)$$

trong đó, $r$ là độ lệch giữa tâm khẩu độ thu và tâm footprint búp sóng quang trên mặt phẳng chứa bộ thu. $h_p(.)$ phần công suất thu được bởi bộ thu, và $A$ là diện tích vùng thu. Công thức (10) có thể được tính gần đúng như sau:

$$h_p\left(r;a\right) \approx A_0 \exp\left(-\frac{2r^2}{\omega_{zeq}^2}\right), \quad (11)$$

trong đó, $A_0 = \left[erf\left(\upsilon\right)\right]^2$ là phần công suất thu được khi $r=0, \upsilon = \frac{\sqrt{\pi}a}{\sqrt{2}\omega_z}$, và $\omega_{zeq}^2 = \omega_z^2 \frac{\sqrt{\pi}erf\left(\upsilon\right)}{2\upsilon\exp\left(-\upsilon^2\right)}$. $\omega_{zeq}$ là độ rộng búp tương đương tại BS.

Đối với liên kết vô tuyến, giả thiết kênh vô tuyến được mô hình như là kênh có tầm nhìn thẳng LOS. Do vậy, liên kết vô tuyến này chỉ chịu ảnh hưởng của suy hao. Kết quả là, hệ số kênh của kênh vô tuyến được tính như sau:

$$h_w = G_{TX} G_{RX} / P_L^W , \quad (12)$$

trong đó, $G_{TX}$ và $G_{RX}$ tương ứng là hệ số khuếch đại của anten phát và thu; $P_L^W$ là tổng suy hao liên kết vô tuyến. Tổng suy hao này được tính theo đơn vị $dB$ bởi $P_L^W = 20\log(4\pi f_c d / c) + \gamma d$ , trong đó $d$ là khoảng cách liên kết vô tuyến và $\gamma$ là hệ số suy hao tổng.

### 3.3. Tỉ lệ lỗi bit lượng tử

Tỉ lệ lỗi bit lượng tử được định nghĩa là tỉ số xác suất mà Bob phát hiện sai bit "0" và "1" ($P_{err}$) trên xác suất mà Bob có thể quyết định các bit nhận được là "0" và "1" ($P_{sift}$). Theo đó, QBER có thể được biểu diễn như sau:

$$\mathrm{QBER} = \frac{P_{err}}{P_{sift}} , \quad (13)$$

trong đó, $P_{err}$ và $P_{sift}$ được tính như sau:

$$\begin{aligned} P_{err} &= P_{A,B}(0,1) + P_{A,B}(1,0) \\ P_{sift} &= P_{A,B}(0,0) + P_{A,B}(0,1) + P_{A,B}(1,0) + P_{A,B}(1,1) \end{aligned}, \quad (14)$$

trong đó, $P_{A,B}(i,j)$ là xác suất mà tại một thời điểm bit ở bên Alice là "$i$" nhưng bit bên Bob là "$j$". Xác suất này có thể được tính như là $P_{A,B}(\mathrm{i},\mathrm{j}) = P_A(i)P_{(B/A)}(j|i)$ , trong đó $P_A(i) = 1/2$ và $P_{(B/A)}(j|i)$ là xác suất mà Bob nhận được bit "$j$" trong khi Alice gửi đi bit "$i$". Dựa trên nguyên lý tách sóng hai ngưỡng, xác suất của $P_{(B/A)}(j|i)$ có thể được mô tả gần đúng như sau [25]:

$$\begin{aligned} P_{B|A}(0|0) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2}\right)dy = \frac{1}{2}\mathrm{erfc}\left(\frac{i_0-d_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(0|1) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2}\right)dy = \frac{1}{2}\mathrm{erfc}\left(\frac{i_1-d_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(1|0) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{d_1}^{\infty}\exp\left(-\frac{(y-i_0)^2}{2\sigma_n^2}\right)dy = \frac{1}{2}\mathrm{erfc}\left(\frac{d_1-i_0}{\sigma_n\sqrt{2}}\right) \\ P_{B|A}(1|1) &= \frac{1}{\sigma_n\sqrt{2\pi}}\int_{-\infty}^{d_0}\exp\left(-\frac{(y-i_1)^2}{2\sigma_n^2}\right)dy = \frac{1}{2}\mathrm{erfc}\left(\frac{d_1-i_1}{\sigma_n\sqrt{2}}\right) \end{aligned}, \quad (15)$$

Để điều chỉnh được giá trị của hai ngưỡng tách sóng, hệ số $k$ được thêm vào và hai giá trị ngưỡng được định nghĩa như sau:

$$\begin{aligned} d_0 &= E\left[i_0\right] - k\sqrt{\sigma_n^2} \\ d_1 &= E\left[i_1\right] + k\sqrt{\sigma_n^2} \end{aligned} , \quad (16)$$

trong đó $E[i_0]$ và $E[i_1]$ là giá trị trung bình của $i_0$ và $i_1$.

### 3.4. Tốc độ khóa bí mật

Tốc độ khóa bí mật Egodic, kí hiệu là S, cho biết mức độ bảo mật của hệ thống đề xuất. Tốc độ khóa bí mật được định nghĩa là tốc độ truyền dẫn tối đa mà Eva không thể giải mã bất kỳ thông tin nào, được tính như sau:

$$S = I(A;B) - I(A;E), \quad (17)$$

trong đó, $I(A;B)$ và $I(A;E)$ là lượng thông tin chia sẻ giữa Alice và Bob, và giữa Alice và Eve tương ứng. Với giả thiết rằng xác suất truyền bit "0" và "1" là xảy ra bằng nhau, thông tin chia sẻ giữa Alice và Bob có thể được tính như sau [25]:

$$I(A;B) = p\log_2(p) + (1-p-q)\log_2(1-p-q) - (1-q)\log_2(1-q) + 1 - q, \quad (18)$$

trong đó, $p = P_{A,B}(0,0) = P_{A,B}(1,1)$ and $q = P_{A,B}(0,x) = P_{A,B}(1,x) = 0.5 - P_{A,B}(0,0) - P_{A,B}(0,1)$.

Thông tin chung giữa Alice và Eve có thể tính bằng [25]:

$$I(A;E) = 1 + p_e\log_2(p_e) + (1-p_e)\log_2(1-p_e), \quad (19)$$

trong đó, $p_e$ là xác suất mà Eve phát hiện đúng các bit được truyền đi từ Alice, có thể được tính là $p_e = 0.5 - P_{A,E}(0,1) = 0.5 - P_{A,E}(1,0)$. Ngoài ra, xác suất lỗi của Eve được tính như sau:

$$\mathrm{QBER}_{Eve} = P_{A,E}(0,1) + P_{A,E}(1,0), \quad (20)$$

trong đó, $P_{A,E}(0,1)$ và $P_{A,E}(1,0)$ là xác suất lỗi mà Eve quyết định sai bit nhận được từ Alice. Giả sử rằng Eve sử dụng tách sóng đơn ngưỡng, đây là mô hình tách sóng thường dung cho máy thu quang. Xác suất lỗi có thể được tính như sau [23]:

$$P_{A,E}(0,1) = P_A(0)P_{E|A}(1|0) = \frac{1}{4}\mathrm{erfc}\left(\frac{d_E - i_0}{\sigma_n\sqrt{2}}\right), \quad P_{A,E}(1,0) = P_A(1)P_{E|A}(0|1) = \frac{1}{4}\mathrm{erfc}\left(\frac{i_1 - d_E}{\sigma_n\sqrt{2}}\right), \quad (21)$$

trong đó $d_E = 0$ là ngưỡng tách sóng tại bộ thu của Eve (như Hình 4).

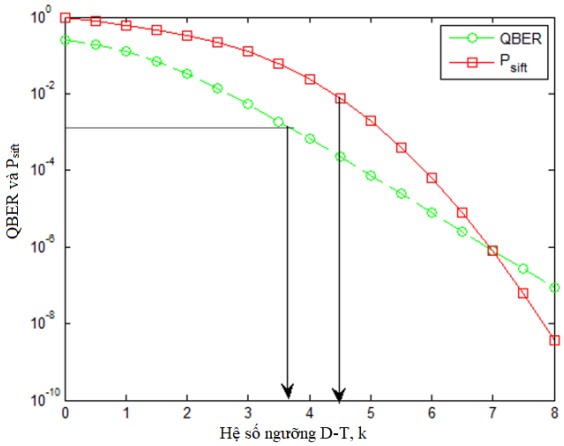
## IV. KẾT QUẢ KHẢO SÁT HIỆU NĂNG

Trong phần này, các kết quả khảo sát hiệu năng sẽ được trình bày dựa trên các công thức giải tích trong phần trên. QBER tại bộ thu của Bob và của Eve được xem xét phụ thuộc vào rất nhiều tham số của hệ thống như hệ số $k$, công suất phát quang ($P_p$). Ngoài ra, tốc độ khóa bí mật cũng được xem xét. Các tham số và hằng số được liệt kê trong Bảng 1.

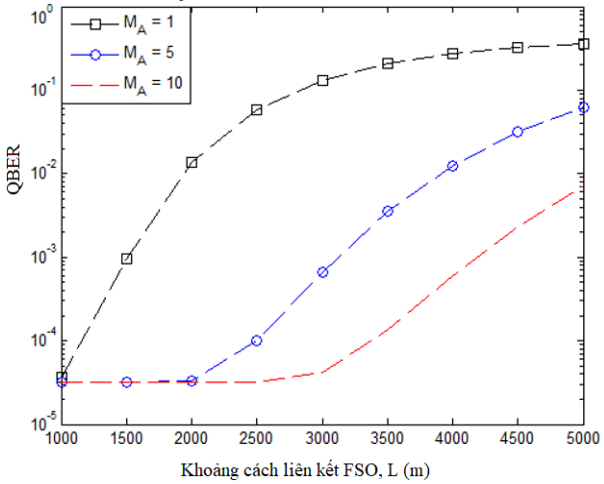
*Bảng 1. Tham số hệ thống và hằng số*

| Tên tham số, hằng số | Ký hiệu | Giá trị |
|---|---|---|
| ***Các tham số và hằng số chung*** | | |
| Hằng số Boltzmann | $K$ | $1.38\times10^{-23}$ $WHz^{-1}K^{-1}$ |
| Điện tích điện tử | $q$ | $1.6\times10^{-19}$ C |
| Vận tốc ánh sáng | $c$ | $3\times10^{8}$ m/s |
| Nhiệt độ Kenvin | $T$ | 300 K |
| Bước sóng | $\lambda$ | 1550 nm |
| Hệ số tạp âm | $F_n$ | 5 dB |
| ***Các tham số kênh FSO*** | | |
| Tốc độ bit | $R_b$ | 1 Gbps |
| Hệ số khuếch đại thấu kính phát | $G_{TX}^{CS}$ | 10 dB |
| Hệ số khuếch đại thấu kính thu | $G_{RX}^{BS}$ | 10 dB |
| Hệ số cấu trúc chỉ số khúc xạ | $C_n^2$ | $10^{-15}m^{-2/3}$ |
| Đáp ứng của APD | $\Re$ | 0,6 A/W |
| Tỉ lệ hệ số i-ôn hóa | $k_A$ | 0,7 |
| Hệ số suy hao | $a_L$ | 0.1 $km^{-1}$ |
| Bán kính chùm quang tại 1 km | $\omega_z$ | 2 m |
| Phương sai dao động | $\sigma_s$ | 10 cm |
| Bán kính thu | $2a$ | 20 cm |
| ***Các tham số RF*** | | |
| Tần số sóng mang | $f_c$ | 28 GHz |
| Băng thông | $B$ | 500 MHz |
| Hệ số suy hao | $\gamma$ | 4 dB/km |
| Hệ số khuếch đại anten phát | $G_{TX}$ | 15 dB |
| Hệ số khuếch đại anten thu | $G_{RX}$ | 25 dB |

Trước tiên, việc thiết kế bộ thu của Bob được xem xét. Tại đây, QBER và $P_{sift}$ được điều khiển để đáp ứng các mục tiêu yêu cầu. Cụ thể là, $P_{sift}$ nên lớn hơn hoặc bằng $10^{-2}$ để Bob có thể nhận được khóa từ Alice với tốc độ Mbps khi tốc độ truyền dẫn đạt đến Gbps. Ngoài ra, QBER được giữ thấp hơn hoặc bằng $10^{-3}$ để lỗi bit có thể được khôi phục nhờ các mã sửa lỗi. Trong Hình 5, QBER được khảo sát phụ thuộc vào hệ số hai ngưỡng khi công suất phát quang $P_p = 0$ dBm, hệ số nhân của APD $M_A = 5$, khoảng cách liên kết FSO $L = 3$ km, và khoảng cách liên kết vô tuyến $d = 500$ m. Để đáp ứng được các mục tiêu trên, hệ số ngưỡng nên nằm trong dải 3.7 và 4.5.



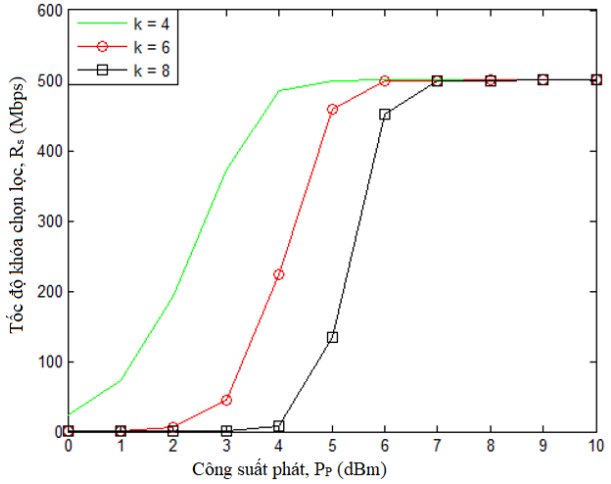

*Hình 5.* QBER và $P_{sift}$ tại phía Bob phụ thuộc vào hệ số ngưỡng khi $P_p = 0$ dBm, $L = 3$ km, và $d_{AB} = 500$ m.



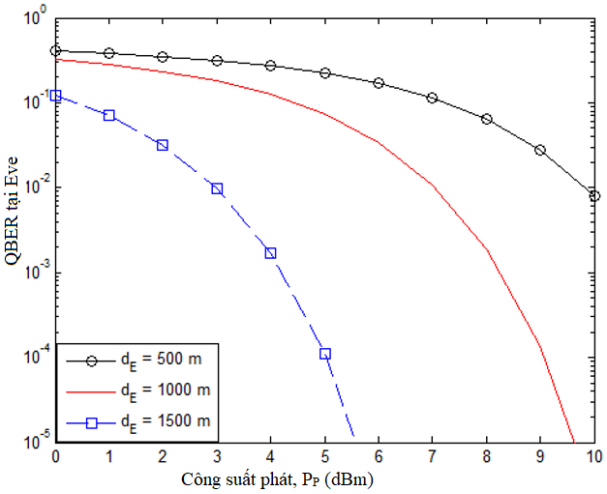

*Hình 6.* QBER tại phía Bob phụ thuộc vào khoảng cách liên kết FSO, L khi $P_p = 0$ dBm, k = 4, và d = 500 m.

Khoảng cách liên kết FSO cũng là một tham số cần khảo sát khi thiết kế hệ thống vì tham số này ảnh hưởng lớn đến hiệu năng hệ thống. Trong Hình 6, tỉ lệ lỗi bit lượng tử được khảo sát phụ thuộc vào khoảng cách liên kết FSO và hệ số nhân của bộ tách quang APD trong trường hợp công suất phát quang ở CS là 0 dBm, khoảng cách vô tuyến là 500 m và hệ số ngưỡng bằng 4 (nằm trong dải khảo sát ở kết quả trên). Như chỉ ra trong Hình 6, khoảng cách liên kết FSO bị giới hạn để đạt được QBER nhỏ hơn hoặc bằng $10^{-3}$. Tuy nhiên, khi hệ số khuếch đại của APD tăng, khoảng cách liên kết FSO được cải thiện đáng kể. Cụ thể là, khi tăng hệ số nhân của APD từ 5 lên thành 10, khoảng cách liên kết FSO được kéo dài thêm 1000 m. Hơn nữa, nếu sử dụng bộ thu là PD ($M_A$ = 1) thì khoảng cách này bị giới hạn nhỏ hơn 1500 m để đạt được mục tiêu thiết kế.

Tiếp theo, tốc độ khóa chọn lọc ($R_s$) được khảo sát. Tốc độ khóa chọn lọc $R_s$ được tính là $R_s = P_{sift}R_b$ với $R_b$ là tốc độ bit của hệ thống. Hình 7 mô tả tốc độ khóa chọn lọc biến thiên theo công suất phát quang khi $M_A$ = 5, $L$ = 3 km, và $d$ = 500 m. Ba giá trị của hệ số ngưỡng được xem xét bao gồm $k$ = {4; 6; 8}. Tốc độ khóa chọn lọc tối đa có thể đạt được là 500 Mbps, chiếm 50% tốc độ bit của hệ thống. Do lỗi bit gây ra bởi các tham số lớp vật lý, xác suất chọn lọc có thể xuống dưới 50% và do đó tốc độ khóa chọn lọc nhỏ hơn 500 Mbps. Để tăng tốc độ khóa chọn lọc, công suất phát quang phải tăng hoặc hệ số ngưỡng phải giảm. Ta có thể thấy rằng trường hợp $k$ = 4 cho tốc độ khóa chọn lọc cao nhất khi so ở cùng mức công suất phát ví dụ như 3 dBm. Điều này phù hợp với kết luận khi khảo sát ở Hình 5, hệ thống cho hiệu năng tốt nhất khi k nằm trong khoảng từ 3.7 đến 4.5.



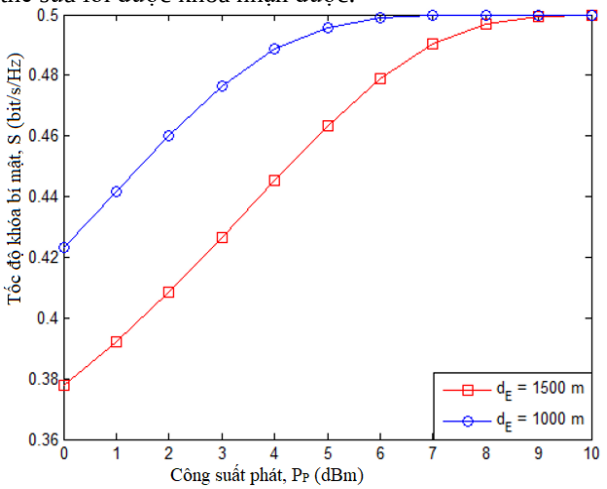

*Hình 7.* Tốc độ khóa chọn lọc phụ thuộc vào công suất phát khi $L$ = 3 km, $d$ = 500 m, $M_A$ = 5.




*Hình 8.* QBER tại Eve phụ thuộc vào công suất phát, khi $L$ = 3 km và $d$ = 500 m.

Trong Hình 8, QBER của Eve được khảo sát phụ thuộc vào công suất phát quang khi $k$ = 4, $L$ = 3 km, d = 500 m và khoảng cách giữa Eve và BS, $d_E$ nhận ba giá trị {500 m, 1000 m, 1500 m}. Rõ ràng rằng, để QBER được giữ thấp hơn hoặc bằng $10^{-3}$ để lỗi bit có thể được khôi phục nhờ các mã sửa lỗi tại Eve, Eve có thể bắt được khóa, công suất phát phải tăng lên khi khoảng cách từ Eve đến BS tăng lên. Tuy nhiên, khi khoảng cách này là quá xa, ví dụ $d_E$ = 1500 m, công suất quang phát phải rất cao (lớn hơn 10 dBm) thì Eve mới đạt được mục tiêu. Như vậy, công suất phát quang của hệ thống có thể được điều chỉnh ở mức nhỏ để Eve không thể thu được khóa với tỉ lệ lỗi bit lượng tử nhỏ hơn $10^{-3}$.

Một tham số hiệu năng nữa của hệ thống cần được khảo sát đó là tốc độ khóa bí mật ergodic. Trong Hình 9, tốc độ khóa bí mật được khảo sát phụ thuộc vào công suất phát quang khi $k$ = 4, $L$ = 3 km, $d$ = 500 m và khoảng cách giữa Alice và Eve nhận hai giá trị là 1000 m và 1500 m. Nhận thấy rằng tốc độ khóa bí mật ergodic tăng khi công suất phát tăng. Do vậy, để đạt được tốc độ khóa bí mật cao thì công suất phát quang phải ở mức cao. Tuy nhiên, khi công suất phát quang cao thì khả năng Eve có QBER thấp và do đó khả năng sửa lỗi của Eve là lớn. Như vậy, khi thiết kế cần phải lựa chọn công suất phát quang sao cho đạt được tốc độ khóa bí mật cao mà Eve không thể sửa lỗi được khóa nhận được.




*Hình 9.* Tốc độ khóa bí mật Ergodic phụ thuộc vào công suất phát khi k = 4, L = 3 km, $d$ = 500 m.

## V. KẾT LUẬN

Bài báo đã đề xuất giải pháp phân phối khóa lượng tử không dây lai ghép FSO và MMW sử dụng điều chế cường độ sóng mang con với tín hiệu BPSK và bộ thu tách sóng hai ngưỡng. Các mô hình giải tích cho các phân tích bảo mật của hệ thống đề xuất được xây dựng. Tỉ lệ lỗi bit lượng tử, tốc độ khóa chọn lọc và tốc độ khóa bí mật biến thiên theo các tham số lớp vật lý được xem xét. Các kết quả khảo sát hiệu năng chứng tỏ rằng hệ thống đề xuất có thể đạt được các mục tiêu bảo mật mong muốn bao gồm QBER nhỏ hơn $10^{-3}$ và tốc độ khóa chọn lọc đạt được tại tốc độ Mbps. Ngoài ra, tốc độ khóa bí mật ergodic có khả năng đạt được tối đa đến 0.5 (bit/s/Hz). Các kết quả cho thấy hệ thống QKD không dây lai ghép là giải pháp hiệu quả để phân phối khóa lượng tử tới các thiết bị di động.

## TÀI LIỆU THAM KHẢO


[1] A. I. Nurhadi and N. R. Syambas, "Quantum Key Distribution (QKD) Protocols: A Survey," Proc. of the 4th *International Conference on Wireless and Telematics* (ICWT), Nusa Dua, 2018, pp. 1–5.

[2] C. H. Bennett and G. Brassard, "Quantum Cryptography: Public Key Distribution and Coin Tossing," *Proc. of the IEEE International Conference on Computers, Systems, and Signal Processing*, Bangalore, India, 1984, pp. 175–179.

[3] H. P. Yuen," Security of Quantum Key Distribution," *IEEE Access*, vol. 4, pp. 724–749, 2016.

[4] A.K. Ekert, "Quantum Cryptography based on Bell's Theorem," *Phys. Rev. Lett.*, vol. 67, no. 6, pp. 661–663, 1991.

[5] F. Grosshans and P. Grangier, "Continuous Variable Quantum Cryptography using Coherent States," *Phys. Rev. Lett.*, vol. 77, no. 2, pp. 513–577, 2002.

[6] Q. Xuan, Z. Zhang, and P. Voss, "A 24 km Fiber-based Discretely Signaled Continuous Variable Quantum Key Distribution Systems," *Opt. Express*, vol. 17, no. 26, pp. 24244–24249, 2009.

[7] Shimizu Kea, "Performance of Long-distance Quantum Key Distribution over 90-km Optical Links Installed in a Field Environment of Tokyo Metropolitan area," *IEEE J. Lightw. Technol.*, vol. 31, no. 1, pp. 141–151, 2016.

[8] P. V. Trinh and A. T. Pham, "Design and Secrecy Performance of Novel Two-way Free-space QKD Protocol using Standard FSO Systems," *IEEE International Conference on Communications* (ICC), Paris, France, 2017, pp. 1–6.

[9] P. V. Trinh, T. V. Pham, N. T. Dang, H. V. Nguyen, S. X. Ng and A. T. Pham, "Design and Security Analysis of Quantum Key Distribution Protocol Over Free-Space Optics Using Dual-Threshold Direct-Detection Receiver," *IEEE Access*, vol. 6, pp. 4159–4175, 2018.

[10] S. Nauerth, F. Moll, M. Rau, C. Fuchs, J. Horwath, S. Frick, and H Weinfurter, "Air-to-Ground Quantum Communication," *Nature Photonics*, vol. 7, pp. 382–386, 2013.

[11] R. Bedington, J. M. Arrazola, and A. Ling, "Progress in Satellite Quantum Key Distribution," *npj Quantum Information*, vol. 3, no. 30, pp. 1–13, 2017.

[12] M. A. Khalighi and M. Uysal, "Survey on Free Space Optical Communication: A Communication Theory Perspective," *IEEE communications Surveys & Tutorials*, vol. 16, no. 4, pp. 2231–2258, June 2014.

[13] M. Gabbi and S. Arnon, "Quantum key distribution by free space MIMO system," *IEEE/OSA J. Lightw. Technol.*, vol. 24, no. 8, pp. 3114–3140, Aug. 2006.

[14] H. V. Nguyen et al., "Network Coding Aided Cooperative Quantum Key Distribution Over Free-Space Optical Channels," *IEEE Access*, vol. 5, pp. 12301–12317, 2017.

[15] P. V. Trinh and A. T. Pham, "Design and secrecy performance of novel two-way free-space QKD protocol using standard FSO systems," *2017 IEEE ICC*, Paris, 2017, pp. 1–6.

[16] Nauerth, S. et al. "Air-to-ground quantum communication," *Nat. Photonics*, vol. 7, pp. 382–386, 2013.

[17] Scheidl, T. et al:, "Quantum optics experiments using the International Space Station: a proposal," *New. J. Phys.*, vol. 15, 043008, 2013.

[18] R. Bedington et al:, "Progress in satellite quantum key distribution," *npj Quantum Information*, vol. 3, no. 30, 2017.

[19] M. Safari and M. Uysal, "Relay-Assisted Quantum-Key Distribution Over Long Atmospheric Channels," *IEEE/OSA J. Lightw. Technol.*, vol. 27, no. 20, pp. 4508–4515, Oct.15, 2009.

[20] Minh Q. Vu, Ngoc T. Dang, Anh T. Pham, "HAP-Aided Relaying Satellite FSO/QKD Systems for Secure Vehicular Networks", 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, 2019.

[21] G. Agrawal 2010. *Fiber-optic Communication Systems* (4th edition). John Wiley and Sons Ltd., New York, USA.

[22] H. Hemmati, *Near-earth laser communications*, CRC Press, 2009.

[23] B.E.A. Saleh and M.C. Teich, *Fundamentals of Photonics*, NewYork: Wiley, 1991.

[24] 3GPP TR 38.811, "Study on new radio (NR) to support non-terrestrial networks," v1.0.0, 2018

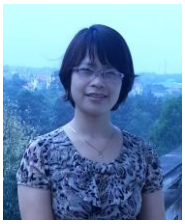
[25] Takuya Ikuta and Kyo Inoue, "Intensity modulation and direct detection quantum key distribution based on quantum noise", new journal of physics, 2015.

[26] O. Simeone, I. Stanojev, S. Savazzi, Y. Bar-Ness, U. Spagnolini, and R. Pickholtz, "Spectrum leasing to cooperating secondary ad hoc networks," *IEEE Journal on Selected Areas in Communication*, vol. 26, no. 1, pp. 203-213, Jan. 2008.


## A SOLUTION OF QUANTUM KEY DISTRIBUTION OVER HYBRID WIRELESS SYSTEM USING FSO AND MMW

***Abstract*** - In this paper, we propose a solution of quantum key distribution over hybrid wireless system using FSO and MMW. Quantum keys from the sender (Alice) are transmitted via the FSO channel to the base station (BS) and then forwarded to mobile stations (Bob) via radio channel. The QKD protocol is implemented based on the subcarrier intensive modulation (SIM) using binary phase shift key (BPSK) for encoding and the dual-threshold receiver for decoding. The performance of proposed QKD system in terms of the quantum bit-error rate (QBER) is analyzed under the influence of physical layer parameters coming from the receiver, FSO channel and MMW radio channel. The numerical results confirm the feasibility of the proposed QKD system.

***Key words*** - Quantum key distribution (QKD), Free-space Optics (FSO), Subcarrier intensive modulation (SIM), Quantum bit-error rate (QBER).



**Phạm Anh Thư** tốt nghiệp đại học tại Học viện công nghệ Bưu chính Viễn thông (PTIT) năm 2003 và tốt nghiệp thạc sĩ chuyên ngành kỹ thuật Viễn thông tại Học viện công nghệ Hoàng gia Melbourne (RMIT), Australia năm 2008. Năm 2019, cô đã nhận bằng Tiến sĩ chuyên ngành kỹ thuật viễn thông tại Học viện công nghệ Bưu chính Viễn thông. Hiện nay cô là giảng viên tại khoa Viễn thông 1, Học viện công nghệ Bưu chính Viễn thông. Lĩnh vực nghiên cứu bao gồm kĩ thuật mạng, truyền song vô tuyến qua sợi quang, mạng băng rộng và an ninh mạng.

**Đặng Thế Ngọc** tốt nghiệp đại học tại Đại học Bách Khoa Hà Nội năm 1999, và tốt nghiệp thạc sĩ tại Học viện công nghệ Bưu chính Viễn thông vào năm 2005. Anh nhận bằng Tiến sĩ chuyên ngành kĩ thuật và khoa học máy tính tại đại học Aizu Nhật Bản năm 2010. Hiện nay anh là phó giáo sư giữ chức vụ Trưởng Bộ môn Thông tin vô tuyến thuộc Khoa Viễn thông 1, Học viện công nghệ Bưu chính Viễn thông. TS. Ngọc từng làm nghiên cứu viên mời tại Đại học Rennes 1 (CH Pháp) và Đại học Aizu (Nhật Bản). Lĩnh vực nghiên cứu của anh gồm liên quan đến lý thuyết truyền thông đặc biệt về mô hình, thiết kế, và đánh giá hiệu năng của các hệ thống truyền thông quang không dây, RoF, CDMA quang và phân phối khóa lượng tử.